Cyber Gray Space Deterrence

By Richard Andres

During the past few years, adversaries of the United States have begun to use their militaries to test U.S. resolve through innovative methods designed to bypass deterrent threats and avoid direct challenges.[1] These "gray space campaigns" are specifically designed to allow adversaries to achieve their goals without triggering escalation by making retaliation difficult. China demonstrated this with its attempt to seize control of the South China Sea through its island building program, as did Russia with its effort to foment insurgency in eastern Ukraine through the use of "little green men."

Cyberattacks often are less flamboyant than the physical campaigns in the South China Sea or Eastern Ukraine, but they may cause more damage to U.S. economic and national security interests. Administration officials, for example, have estimated that China's intellectual property (IP) theft program costs the U.S. economy billions of dollars each year and, despite repeated threats from the United States, the program has persisted for more than a decade. Similarly, despite public threats by the U.S. President and leaders of allied European nations, Russia's cyber-based psychological-political campaign may be increasing in magnitude.

Virtually nothing has been done to increase the credibility of U.S. cyber deterrent threats despite widespread recognition across U.S. policy channels of the potential for cyberattacks to undermine U.S. economic and military security. Reports and strategies have been worried over but then ignored, and draft legislation has repeatedly foundered in Congress. Other than bluster, the only tangible steps the U.S. Government has taken to deter cyberattacks by foreign states has been to indict select soldiers and civilians who launched them.

When asked why the United States has been unable and unwilling to deter cyberattacks, policymakers generally provide two explanations—attribution and fear. As former Director of National Intelligence James Clapper related in his recent testimony before the U.S. Senate:[2]

> *We'll never be in a position to launch a counter attack even if we can quickly and accurately attribute who attacked us … and we're always going to doubt our ability to withstand counter retaliation.*

Dr. Richard Andres is a professor of national strategy at the National Defense University's National War College. Dr. Andres was the 2017 Scholar in Residence at the U.S. National Security Agency and a Special Advisor to the Secretary of the U.S. Air Force. The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy opinion of DOD, or any agency of the U.S. Government. Any appearance of DOD visual information for reference does not imply or constitute DOD endorsement of this work.

Both explanations accurately describe parts of the problem, yet neither offer a satisfying explanation. Although attribution can be difficult, in each of the headline grabbing cases cited earlier the identity of the attacker was known and the attacking government was subjected to diplomatic demarches. Furthermore, while it is true that the United States is more vulnerable to attacks than some of its opponents, it is also the case that the United States arguably has escalation dominance. It would not, for instance, be a great innovation for the United States to threaten economic sanctions against a state attacking through cyberspace. Thus, unless U.S. policymakers choose to restrict their deterrent threats and escalation paths strictly to cyberspace, it is not clear why cyber vulnerabilities should deter our nation from responding to attacks.

The fundamental problem the United States faces in regard to cyber deterrence is that its adversaries calculate that the benefits of their attacks exceed the risks of U.S. retaliation. This perverse incentive exists because the United States has chosen not to make strong enough threats or to back them with the actions that would lead potential attackers to believe the threats are credible. Because the United States almost certainly has the capability to make and back such threats, it has become relatively common to argue that the United States is self-deterred. However, this argument offers little new insight in that all deterrence is *self-deterrence*. To say the United States is self-deterred is merely to say its adversaries have found ways to convince it not to attempt to deter attacks.

A more useful way to frame the problem of U.S. self-deterrence is to think in terms of the specific actions America's adversaries are taking to encourage self-deterrence. The following sections explore the specific benefits adversaries gain from attacking the United States in and through cyberspace and some of the means they use to undermine U.S. deterrence.

The Benefits States Receive from Cyberattacks

During the past three decades, like many other countries, the United States connected virtually everything related to its economy and national security to computer networks and then failed to adequately defend those networks. These actions (or inactions) have created lucrative targets. The value of what cyberattackers can now obtain arguably rivals what, in previous eras, could only have been obtained through territorial conquest. States have discovered they can profit from cyberspace attacks through economic and state espionage, sabotage, and psychological operations.

Economic Espionage

Economic espionage is not new, but a number of developments have increased the importance of this type of vulnerability. First, the overall commercial value of secret information has increased in recent years. In the 1970s, for example, around 80 percent of the value of most U.S. corporations was stored in brick and mortar assets with the remainder contained in intangibles such as trade secrets and intellectual property. Today, roughly 20 percent of the value of most U.S. businesses resides in physical assets and 80 percent in information assets. A number of states use their intelligence agencies to loot their adversaries' businesses, but none come close to China either in terms of volume of commercial secrets taken or its ability to disseminate stolen intellectual property (IP) to its own commercial firms. The profit China derives from stolen commercial secrets is so great that it likely accounts for a large portion of China's often touted miraculous economic growth.

State Espionage

Like commercial espionage, traditional state espionage has also benefited greatly from cyber tools. With most state secrets now online and often lightly defended, the ability to hack secure government systems allows adversary states to garner information thousands of times more efficiently than in the past. Moreover, in the information age, the value of those secrets is often greater than in the past. This is particularly true of intelligence regarding military affairs in as much as modern military assets are generally controlled via computer chips and networks. Whereas, in the past, espionage allowed spies to learn about the location and behavior of an opponent's assets, in the current era, stolen encryption keys and related security protocols have the potential to allow their possessor to disable, destroy, or even control an adversary's hardware from a computer terminal thousands of miles from the front line. Thus, nations sometimes gain extraordinary benefits from their espionage programs.

Sabatoge

Military and civilian critical infrastructure in most industrial countries is now attached to digital networks. The vulnerability of these assets to cyberattack provides significant incentives for nations to hack them, and both commercial enterprises and military organizations regularly complain that they have discovered adversary state-originating malware on their systems. In some cases, such as Iran's attack on Saudi Aramco, U.S. banks, and a U.S. dam (2011–13), the attacks involved both gaining access to a system and doing damage.[3] However, it is more common for states to deploy malware designed to gain access to targeted systems in order to hold it at risk against potential future contingencies.[4] These hacks have the potential to do damage on par with nuclear weapons. An attack that took down the U.S. electrical grid for an extended period of time, for example, could lead to millions of deaths through starvation and related causes.[5] This ability to hold civilian and military infrastructure at risk provides a cheap substitute for conventional power projection armaments. Moreover, as the former Director of National Intelligence's comments suggest, such capabilities do not have to be executed to provide their holders with substantial coercive bargaining power.

Pyschological Operations

The first major psychological cyber operations were conducted by the United States against a range of autocratic allies and adversaries. In 2010, then Secretary of State Hillary Clinton described her intent to oppose autocracies' ability to restrict information within their borders with the intent of furthering democracy.[6] Russian and Chinese leaders believed Clinton's main goal was to foment regime change in their nations and they repeatedly attributed the rebellions associated with the Arab Spring to this policy. China responded with the internal information control and suppression programs associated with the so called Great Firewall of China. Russia, which was less concerned than China about internal stability, retaliated by developing an outward facing cyber-psychological-political capability that it used to delegitimize its opponents' governments and foment mistrust in its adversary alliances. Russia appears to receive substantial security benefits from its cyber-psychological programs.

American Reticence to Threaten Retaliation

Given the benefit various adversaries receive from their cyber programs, it is apparent that, in some cases, the United States would have to be willing to threaten substantial costs to force attackers to abandon their operations. The problem is not one of capability for the United States—it has the resources and ability to impose such costs. For example, even if China's economy gains a great deal from IP theft, China almost certainly depends even more on trade with the United States. Russia undoubtedly values what its psychological operations are doing to weaken the West, but Moscow probably is even more afraid of the types of psychological operations and economic sanctions the United States could impose on Russia should it chose to expend the resources.

Rather, the fundamental problem is that U.S. policymakers are unwilling to pay the costs. From the perspective of traditional deterrence theory, America's reluctance to seriously attempt to deter cyberattacks is puzzling. If the cost of inaction is as high as U.S. policymakers claim to believe, then why do they consistently fail to deploy threats of equally costly retaliation? The first part of the answer is simple—U.S and foreign decisionmakers realize that to follow through with threats would be costly to the United States. A trade war with China might destroy China's economy but would also damage the U.S. economy, and a war of psyops with Russia might seriously damage the United States' relationship with many other nations. But these answers only explain part of the problem. Diplomatic bargaining is basic to international diplomacy. In most cases states are able to use a combination of threats and compromises based on their relative strength and diplomatic ability. In as far as the United States is far stronger in every way than its attackers, it is odd that it has been unable to defend itself.

Methods Attackers Use to Reduce the Risk of U.S. Retaliation

To understand America's reticence to make strong and credible deterrent threats, it is helpful to understand the tactics attackers use to undermine deterrence. A portion of these methods could apply to any type of gray space operation, while some are specific to cyber conflict.

Concealing Attribution

The first and most well-known method attackers use to dampen the threat of retaliation involves concealment of their identity. Because of the nature of cyberspace, attackers can often disguise the origin of their attacks or make the attacks appear to come from a third party. Even when a defender is able to trace the attack to a geographical location, it is often impossible to prove that the individuals at that location were acting on behalf of the government; states regularly conceal attacks behind facades of criminal organizations and patriotic militias. Even when the attackers can be linked to their governments, it is seldom possible to back such claims with the kind of evidence that would stand up in court or in the court of public opinion, and even when such evidence is available, providing it could reveal sensitive sources. Beyond this, attribution problems create incentives for third party nations to conduct false flag attacks designed to provoke conflicts between rivals. Knowing that this incentive exists, defenders have difficulty trusting even apparently clear evidence if acting on it would lead to conflict with the suspected attacker. In sum, even when defenders are relatively confident that they know the identity of an attacker, attribution problems create plausible deniability that can undermine the willingness to retaliate.

Concealing the Cost of the Attack

A second method regularly employed by attackers is to attempt to conceal the value of the attack. Hackers typically attempt to conceal the attack in its entirety. If an attack is discovered by the victim, hackers attempt to conceal the magnitude of the attack. Beyond this, however, the value of espionage, sabotage, and psychological operations is difficult to assess. When IP is stolen, it is not stolen in the traditional sense; rather, it is copied by the thief. It is difficult to assess the harm posed by IP theft, particularly when the evidence mainly resides in the territory of the pirating government. Not only do pirate states not cooperate with investigators, they often build elaborate domestic

The Defense Advanced Research Projects Agency's Plan X program is a foundational cyberwarfare program whose engineers are developing platforms DOD will use to plan for, conduct and assess cyberwarfare in a manner similar to that of kinetic warfare. (DARPA)

institutions specifically designed to disguise their actions. China, for example, has created a massive system of institutions and laws to launder stolen IP and "reinvent" it at home. Such techniques make it difficult to know when a cyberattack has occurred, to ascertain the magnitude and duration, and to assess the economic, security, or political costs—thereby complicating a defender's calculations when attempting to formulate deterrent threats.

Avoiding Symbolic Triggers

Cyberattackers regularly strike in ways that circumvent key psychological, cultural, and legal triggers. In democracies, acting on deterrent threats often requires public support. While national security professionals may be able to respond rationally to calculations, energizing the public often requires appealing to symbols. For instance, when Japan attacked U.S. battleships at Pearl Harbor in 1941, or when al-Qaeda attacked the World Trade Center and Pentagon in 2001, those actions triggered psychological reactions in the American public that had little to do with the economic and military effects on national security. In such cases, the public responds at least as much to fire, smoke, and casualties as to calculations about national interests. If Japan or al-Qaeda had attacked using computer viruses, U.S policymakers might not have gained enough public support to take the country into costly wars. Such dynamics incentivize attackers to stay clear of actions that are likely to trigger emotional responses. This tactic undermines the credibility of potential deterrent threats by requiring defending policymakers to make their case without the ability to appeal to the range of symbolic actions usually required to mobilize the public.

Using Asymmetrical Attacks

In deterrence bargaining, one of the central methods states use to signal intent and contain escalation involves asymmetric retaliation. The United States maintains a variety of instruments that provide it with escalation dominance in most arenas of competition, and Washington typically responds to hostile diplomatic action with diplomatic tools, economic action with economic tools, and military action with military tools. Understanding this dynamic, cyberattackers often attempt to attack the United States asymmetrically, in venues in which it cannot easily respond in kind. For example, China steals IP from the United States knowing that it has virtually no IP that the United States can steal in retaliation; it does not, however, attempt to undermine the legitimacy of the U.S. Government because it understands that the United States would most likely have symmetrical escalation dominance in such a contest. While the United States could threaten to retaliate against cyberattacks asymmetrically through economic sanctions or military threats, there is a significant chance that such actions would appear escalatory, disproportionate, or otherwise inappropriate to the American public or the international community. Consequently, as James Clapper alluded to in his testimony, such attacks complicate deterrence.

Employing Strategic Use of Time and Decision Cycles

In the United States, political leaders face regular elections and generally have short strategic horizons. This dynamic makes the United States particularly vulnerable to salami-slicing tactics. The idea is that an adversary can make as many small attacks as it likes, so long as the total value of the attacks remains beneath a certain threshold during a U.S. policymaker's decision cycle. A U.S. President may be aware that a decade-long campaign by Russia to infiltrate critical infrastructure would have consequences sufficiently dire to justify retaliation; but during any two year period, the results are not serious enough to justify a serious response. So long as elected officials think in terms of election cycles and attackers restrict the damage they do within these cycles they will be free to generate substantial long term results while minimizing the chances of retaliation.

Infiltrating and Manipulating

The United States is an open society, which means even its adversaries are allowed to attempt to influence or compromise the integrity of U.S. policymaking institutions. Russia and China spend large sums to hire highly respected former government officials with a track record of China or Russia bashing to lobby on their behalf; neither country has had trouble finding such officials.[7] China routinely sends hundreds of thousands of students abroad to increase its influence and access, while Russia regularly bribes and blackmails.[8]

Appealing to Reputation

When policymakers calculate how they will respond to an attack, they are often as concerned with their state's reputation as with the cost of the attack. A state that has a reputation for not retaliating against small attacks may come to be seen as an easy target for third parties. Thus, leaders might be willing to pay costs and take risks to avoid small losses that are disproportional to the apparent stake in a dispute. To the extent that cyberattacks are secret, however, this effect is dampened. If a defender loses something from a cyberattack and no one beyond the attacker and defender is aware, the defender may have a smaller incentive to worry about how an unanswered attack will affect its reputation.

Gray Space Deterrence

These tactics help to explain why the United States is regularly self-deterred from even attempting to deter cyberattacks. Its attackers have strong incentives to conduct attacks. This means the United States would have to threaten considerable harm to have much chance of deterring the attacks. Acting on such threats would be costly. Every action the attacker takes to reduce America's confidence lowers its willingness to make or act on costly threats.

To take a fanciful example, if a U.S. decisionmaker assessed that an adversary was conducting an attack on critical infrastructure from which it would eventually gain one billion dollars' worth of security, she might be willing to threaten the suspected attacker with sanctions that would cost the United States one billion dollars to execute. However, if she was only 80 percent confident that she had identified the actual attacker, she might only be willing to threaten sanctions that would cost the United States $800 million to execute. If, beyond this, she was only 80 percent confident that the attacks were truly having the assessed effect, she might only be willing to threaten sanctions costing $600 million. Further, if she was only 80 percent certain the public would see the threat as serious (given the lack of fire, smoke, or loss of life) her cost tolerance might drop to $400 million. If she feared that an asymmetric response, such as economic sanctions, would be costly to the United States' reputation, she might only be willing to bear $200 million in costs. If she believed that only part of the entire billion dollar price tag for the attack would accrue during her time in office, it might be preferable to wait and allow her successor to take the political risk of making the threat. Even if she were willing to take action, her belief in the efficacy of lobbyists acting on behalf of the attacker would further erode her confidence and willingness to place her reputation and political capital behind the policy. If she persisted despite these obstacles and the attacker did not assess that the cost of the sanctions would be higher than the one billion dollars in benefits it was gaining from the attacks, there is a good chance that it would not be deterred.

Real world cases are not as clear cut but this example helps to illustrate the calculations attackers and defenders must make in cyber conflict. If attackers attempted to use their cyber weapons without using such psychological tactics, it would not be particularly hard to deter them. Moreover, the success of these tactics is not entirely dependent on attribution problems or fear of counter-retaliation. Even in cases where the United States has identified attackers and done a good job of assessing the harm caused by their attacks, other dynamics have reduced its confidence to such an extent that decisionmakers have almost uniformly chosen not to act.

Conclusion

Most work on cyber deterrence concludes by advocating better defenses—this is excellent advice, but has so far failed to do much to reduce losses. A bolder approach would be to address each of the psychological tactics attackers employ. What is needed are improved ways to attribute attacks; study the actual cost of attacks; raise public understanding of those costs that do not result in obvious kinetic destruction; develop deterrence policies that operate across election cycles; and expose adversary attempts to illegally (and legally) influence U.S. domestic institutions. Such approaches would mark a departure from current policy but have the potential to undermine adversaries' psychological tactics and improve America's ability to deter cyberattacks. PRISM

Notes

[1] See for instance: Hal Brands, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, February 5, 2016, available at < https://www.fpri.org/article/2016/02/paradoxes-gray-zone/>; Michael Mazarr, "Mastering the Gray Zone: Understanding a Changing Era of Conflict," United States Army War College Press, December 2, 2015, available at < https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303>; Frank Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," *Heritage Foundation*, 2016; Joseph Votel, et al, "Unconventional War in the Gray Zone," *Joint Forces Quarterly*, 1st Qtr, 2016.

[2] Mark Pmerleau, "Lack of Resilience Led to Lack of Cyber Strategy, Says Former DNI," *The Fifth Domain*, May 12, 2017, available at < http://www.fifthdomain.com/2017/05/12/lack-of-resilience-led-to-lack-of-cyber-strategy-says-former-dni/>.

[3] Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," Reuters, March 24, 2016, available at <http://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF>; Jose Pagliery, "The Inside Story of the Biggest Hack in History," *CNN Tech*, August 5, 2015, available at <http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html>; Mark Thompson, "Iranian Cyber Attack on New York Dam Shows Future of War," TIME, March 24, 2016; Andy Greenber, "How an Entire National Became Russia's Test Lab," *Wired*, June 20, 2017, available at <https://www.wired.com/story/russian-hackers-attack-ukraine/>.

[4] Geoffrey Ingolsoll, "Defense Science Board Warns of Existential Cyber Attack," Business Insider. March 6, 2013.

[5] Department of Defense, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics Washington, D.C. 20301-3140, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013.

[6] Elizabeth Dickinson, "Internet Freedom: The Prepared text of U.S. of Secretary of State Hillary Rodham Clinton's Speech," delivered at the Newseum in Washington, D.C. *Foreign Policy*. January 21, 2010.

[7] For a good analysis of China's methods, see: Richard Daft, *Organization Theory and Design*, Cengage Learning, 2006,165. On Russia, see: Garrett M. Graff, "A Guide to Russia's High Tech Tool Box for Subverting US Democracy," *Wired*, August 13, 2017, available at <https://www.wired.com/story/a-guide-to-russias-high-tech-tool-box-for-subverting-us-democracy/?mbid=social_fb_onsiteshare>.

[8] John Garnaut, "Chinese Spies at Sydney University," The Sydney Morning Herald, April 21, 201, available at <http://www.smh.com.au/national/chinese-spies-at-sydney-university-20140420-36ywk.html#ixzz312tdddmi>.

Photos

Page 90: Idaho National Laboratory. From <https://www.flickr.com/photos/30369883@N03/7900490132/>. Licensed under Creative Commons Attribution 2.0 Generic License <https://creativecommons.org/licences/by/2.0/deed.edn>. Photo unaltered.

Page 95: DARPA. Available at < https://www.defense.gov/News/Article/Article/758219/darpas-plan-x-gives-military-operators-a-place-to-wage-cyber-warfare/>.